September 10, 2015 Volume 8, Issue 17

Blue Top Newsletter

Upcoming Meetings and Training

Meeting/Training	Date & Time (EST)	Location	Dial-In Info
User Group	Tue, Sep 15 9:00 to 12:00	GSA Central Office 1800F St. NW Conference Rm 6044	888-455-1864 Passcode: 5887966
ICAM Day: Make a Connection!	Thu, Oct 1 8:00 to 4:00	GSA Central Office 1800F St. NW	No Telecon Provided
CAB	Thu, Oct 8 9:30 to 12:00	Grant Thornton 333 John Carlyle Dr., Alexandria, VA 4th Fl. Conf. Rm	No Telecon Provided
Registrar Refresher Training	Thu, Oct 8 2:30 to 3:30	Telecon	888-455-1864 Passcode: 3611044
Registrar Classroom Training	Wed and Thu Sep 16-17 Oct 14-15 Nov 18-19 Dec 9-10	HP Chantilly, VA	Contact Jim Schoening for information or to Register

ICAM Day: Make a Connection!

GSA is pleased to announce that registration is open for the Fall 2015 ICAM Information Sharing Day on October 1, 2015. The motto of this year's ICAM Day is Make a Connection! This all day event will feature panel discussions, interactive breakout sessions, and a vendor expo. Listen to government leaders discuss recent successes and future opportunities on advancing ICAM implementations to meet government-wide priorities while you network with fellow members of the federal ICAM community. There is no cost associated with registration for ICAM Day sessions, but space is limited! Please register as soon as possible for the event, including your preferred breakout sessions.

For more information click here.

GSA

USAccess Program

Special Points of Note:

Now found on www.fedidcard.gov:

> Service Order Requests and Test Card Orders

> Role Holder Web Based Training Registration

> Deployment Activities and USAccess Center Status Alert

> Contact Ken Bandy (Kenneth.bandy@gsa.gov) to be added to User Group (UG) distribution list.

> Contact Jim Schoening (jim.schoening@gsa.gov) for Registrar Classroom Training sign up

Inside this issue:

Monthly Maintenance Fee to Remain Unchanged in FY16

The Monthly Maintenance Fee will not escalate in FY16. The rate will remain at $3.45 a month.

User Group Meetings Moving to Wednesdays

Starting in October, USAccess User Group Meetings will be moving to the **third Wednesday** of the month. The final Tuesday User Group will be held on September 15. The first Wednesday User Group will be on October 21. Location and teleconference information remain the same.

Dual Interface/Coil Cards to be removed from Approved Products List (APL) December 2015

This is a reminder to announcements we made last year regarding dual interface/coil cards being removed from the FICAM APL.

The GSA Office of Government Policy (OGP) notified us last year that the dual interface cards issued by the USAccess Program will be removed from the FICAM APL. Initially OGP stated that the dual interface cards would be removed from the APL in December 2014. But at our request, they extended the deadline to December 2015 to accommodate USAccess Program customers.

Removal of these dual interface cards from the APL means the USAccess Program can no longer print new dual interface credentials for a USAccess customer starting in January 2016. Dual interface cards that are printed (but not activated) before APL removal in December 2015 can still be activated, and any existing active dual interface cards in the field will not be terminated and will remain active until the card expiration date printed on the front of the card.

The GSA MSO realizes that several Agency customers use dual interface cards with their existing PACS/LACs systems, and discontinuing this type of PIV credential has impact on Agency IT infrastructures. The MSO reached out to impacted Agencies last year and provided a list of Agency credential holders who were issued a dual interface credential on request. Please contact Matt Arnold at matthew.arnold@gsa.gov if you have questions.

Reminder — UPN Password Resets Needed on Fixed Workstations

As part of the project this past Spring/Summer to replace Windows XP USAccess fixed enrollment and activation workstations with a Windows 7 machine, all Registrars and Activators were asked to learn their UPN and use it to reset the UPN password (not to be confused with the credential PIN.) This was necessary to enable Registrars and Activators to use their PIV card to log on to their fixed credentialing machines and as a means of **reducing incidents of shared role holder credentials**.

These UPN passwords are set to expire every 90 days, and therefore the first set of passwords must be reset. Registrars and Activators won't be prompted ahead of the expiration date to reset the password. Rather, they will see a "your password has expired" message when attempting to log in to their fixed enrollment or activation machine.

Registrars and Activators who see this password expired message during workstation log on should follow the steps outlined in a document that was posted on TRACKS in the Training section of the portal. The document is called *Guidance on resetting UPN Password on Fixed Workstations*. This document was also posted as an advisory on the home page of TRACKS on August 6. It contains instructions similar to the steps Registrars and Activators completed to reset their UPN passwords during the Windows 7 workstation replacement process.

The USAccess Help Desk is familiar with this document and can assist callers if they have issues resetting their UPN password. Please share the guide with your Registrars and Activators so they are familiar with how to reset their UPN password.

Service Enhancements

System Changes Since Last Blue Top

- Maintenance completed as scheduled on Saturday, August 29th.
- Supported Migration to Encrypted SIP Web Service for NARA

Update on intermittent activations the past 2 weeks

We've had several instances of intermittent issues with activations on our light and fixed machines the past 2 weeks. The MSO posted advisories on TRACKS and www.fedidcard.gov and also sent out emails to Agency Leads.

We have engaged our extended HP networking and data center teams to analyze server logs and run through the error messages to identify any trends that will lead us to root cause and a fix. We've also reintroduced a monitoring tool used in the past when experiencing periods of activation slowness and continue to closely monitor the system. Once we identify a fix for the issue, we'll provide an update in a future Blue Top. We appreciate your patience.

Issue with OPM EFTS fingerprint transmissions

We experienced an issue last week where EFTS submissions from USAccess to OPM were not received by OPM between Thursday morning, September 3, 2015 beginning around 9:30am Eastern until Friday evening, September 4, 2015 at 6pm Eastern. We put in a temporary fix on the USAccess system Friday afternoon and transmissions for new packages resumed to OPM on Friday evening.

We also re-submitted any backlogged packages held up during the OPM issue so Agencies should be receiving results per usual from OPM. There should be no duplicate billing for these resubmissions. We're working with OPM to deploy a permanent fix once root cause analysis completes.

Update on Personal Credential Assistance (PCA) upgrade on fixed and Light credentialing workstations

As discussed in previous communications, the MSO plans to migrate USAccess fixed Activation workstations to use the PCA solution to conduct activations and card updates/rekeys. Currently scheduled for a December rollout, PCA will replace the current Unattended and Attended Activation portals on fixed activation machines. This migration will occur on fixed machines (only) using an automated push; no action is needed by the agencies to update the fixed machines.

More details on deployment schedules, role holder responsibilities, training events and documentation availability will be shared in the October User Group and Registrar Refresher training, as well future Blue Tops.

PCA will also be made available for Light workstations via a Light PCA installer, however use of PCA is optional for the Agencies (i.e.; the existing Unattended and Attended Activation portals will still be available for use.)

Planned Changes

For any maintenance downtime periods, please schedule some buffer time to resume enrollment and activation appointments to account for any unanticipated delays in service.

- **Maintenance planned for this Saturday afternoon (3pm-8pm), September 12, 2015.**
  This work is back end data center work as part of our vendor's transition to conduct business as Hewlett Packard Enterprise (previously Hewlett Packard or HP) starting November 1, 2015. While we don't anticipate any downtime for the role holder portals as part of this work, if anything, a role holder may experience a brief intermittent issue between 3pm-8pm Eastern. We will post an advisory to let role holders know of the possible interruption but to plan to work as usual.

- **Maintenance scheduled for week of September 18-20, 2015; Role holders could see intermittent issues**
  This work involves routine security scans that will start Friday evening and run through all day Saturday and Sunday, September 18-20. During this time, role holders may experience delays during the scanning period. TRACKS and www.fedidcard.gov advisories will be posted stating role holders may experience intermittent issues.

- **Maintenance scheduled for Saturday, September 26 from 6am-10pm Eastern and *potential* intermittent issues on Sunday, September 27 all day**

  The Saturday outage period is for standard September maintenance. Advisories will be posted on TRACKS and www.fedidcard.gov and an email sent from www.fedidcard.gov.

  On Sunday, September 27, standard security scans are occurring, so role holders may experience delays during the scanning period. TRACKS and www.fedidcard.gov advisories will be posted stating role holders may experience intermittent issues.

Security Tip

USAccess Account Security—Best Practices

We all know and understand that Government systems require that each user be explicitly identified. The Credential produced for you by USAccess is a key element in establishing your unique ID. Unauthorized use of your credential may expose you and your agency to unnecessary risk. In extreme cases it may also expose you to civil and possible criminal penalties. Examples of unauthorized use can include using someone else's credential – with or without their permission, lending your credential to a colleague or leaving it unattended.

In the event that your credential is lost or stolen it must be reported immediately to protect you and your agency from a possible attack. A failure to immediately report it may also expose you to the penalties previously noted.

As a USAccess credential holder it is **solely your responsibility** for protecting your credential, user ID and password. Your continued vigilance is a primary element in preventing credential misuse by unauthorized users.